

KIBERMAKONDAGI KRIMINOLOGIK TAHDIDLARNING DETERMINATSIYASI

<https://doi.org/10.2861/zenodo.14673475>

Aliev Maxsudjon Anvarovich

O'zbekiston Respublikasi Bosh prokuraturasi huzuridagi Iqtisodiy jinoyatlarga qarshi kurashish departamentining Toshkent shahar boshqarmasi bo'lim boshlig'i

Annotatsiya

Ushbu maqolada kibermakonda sodir etiladigan jinoyatlarning kriminologik xususiyatlari, ularning kelib chiqish sabablari va jamiyatning raqamli xavfsizligiga ta'siri tahlil qilinadi. Muallif kiberjinoyatchilikning latentlik darajasi, transchegaraviy tabiati va viktimologik omillarini huquqiy nuqtai nazardan ko'rib chiqadi.

Kalit so'zlar

kibermakon, kriminologik tahdid, latentlik, viktimologiya, determinatsiya, kiberstalking, raqamli profilaktika.

Аннотация

В данной статье анализируются криминологические характеристики преступлений, совершаемых в киберпространстве, причины их возникновения и влияние на цифровую безопасность общества. Автор рассматривает уровень латентности киберпреступности, её трансграничный характер и виктимологические факторы с правовой точки зрения.

Ключевые слова

киберпространство, криминологическая угроза, латентность, виктимология, детерминатсия, киберсталкинг, цифровая профилактика.

Abstract

This article analyzes the criminological characteristics of crimes committed in cyberspace, the causes of their occurrence, and their impact on the digital security of society. The author examines the latency level of cybercrime, its transboundary nature, and victimological factors from a legal perspective.

Keywords

cyberspace, criminological threat, latency, victimology, determination, cyberstalking, digital prevention.

Axborot texnologiyalarining jamiyat hayotiga jadal kirib borishi jinoyatchilikning an'anaviy shakllari transformatsiyasiga va mutlaqo yangi turdagi kriminologik tahdidlarning paydo bo'lishiga olib keldi. Kibermakon jinoiy faoliyatning yangi markazi sifatida namoyon bo'lib, undagi anonimlik va masofasizlik omillari jinoyat sodir etish mexanizmini sezilarli darajada osonlashtirdi. Ushbu jarayonning dolzarbligi shundaki, virtual makon an'anaviy jinoyatchilikning nafaqat chegaralarini kengaytirdi, balki uning kriminologik determinantlarini ham tubdan o'zgartirdi. Masalan, agar ilgari firibgarlik yoki o'g'rilik jinoyati jismoniy kuch bilan yoki muayyan makonga bog'liq bo'lgan bo'lsa, bugungi kunda "fishing" yoki "vishing" kabi ijtimoiy muhandislik usullari yordamida jinoyatchi dunyoning istalgan nuqtasidan turib, bir vaqtning o'zida minglab qurbonlarga hujum qilish imkoniyatiga ega. Bu holat jinoyatchilikning transchegaraviy tabiatini kuchaytirib, milliy yurisdiksiyalar doirasidagi profilaktika choralari samaradorligini pasaytirmoqda.

Raqamli transformatsiya natijasida yuzaga kelayotgan yana bir muhim kriminologik tahdid – bu davlat va jamiyat uchun muhim ahamiyatga ega bo'lgan axborot infratuzilmalariga qilinayotgan tizimli hujumlardir. Xususan, bank-moliya tizimlariga shifrovchi dasturlar orqali qilinayotgan hujumlar nafaqat iqtisodiy zarar yetkazmoqda, balki ijtimoiy barqarorlikka ham xavf solmoqda. Bu borada "makonlararo o'tish" nazariyasiga ko'ra, jinoyatchilarning virtual muhitdagi anonimligi ularda jazosizlik hissini uyg'otishi natijasida, real hayotda jinoyatdan tiyiladigan shaxslarning ham kibermakonda faol kriminal sub'ektga aylanishi kuzatilmoqda. Masalan, kriminologik tadqiqotlar shuni ko'rsatadiki, kibermakondagi jinoyatlarning aksariyati avval sudlanmagan va ijtimoiy jihatdan "xavfsiz" deb topilgan shaxslar tomonidan sodir etilmoqda, bu esa jinoyatchi shaxsini o'rganishda an'anaviy metodlardan voz kechib, yangi raqamli profillash usullarini joriy etishni taqozo etadi.

Bundan tashqari, Web 2.0 va Web 3.0 texnologiyalarining rivojlanishi voyaga yetmaganlarning viktimizatsiya darajasini keskin oshirdi. Kiberbulling, kiberstalking va onlayn ekspluatatsiya kabi tahdidlar endilikda jismoniy hudud bilan cheklanmay, sutkasiga 24 soat davomida qurbonning ruhiy holatiga ta'sir o'tkazish imkonini bermoqda. Bu jarayonda qurbon va jinoyatchi o'rtasidagi masofaning yo'qligi va axborotning tez tarqalishi jinoyatning latentlik darajasini oshirib, huquqni muhofaza qilish organlari uchun elektron dalillarni to'plash va kvalifikatsiya qilishda murakkab muammolarni keltirib chiqarmoqda. Shu sababli, kibermakondagi kriminologik tahdidlarni tahlil qilishda faqatgina texnik xavfsizlikka emas, balki raqamli makonning ijtimoiy-huquqiy determinantlarini

chuqur o'rganish va shu asosda yangi avlod profilaktika tizimini yaratish bugungi kunning eng dolzarb vazifasi hisoblanadi.

Kibermakondagi zamonaviy tahdidlarning kriminologik tavsifida yuqori darajadagi latentlik, transchegaraviylik va texnik determinatsiya omillari ilmiy hamjamiyat tomonidan jinoyatchilikning yangi avlodini belgilovchi asosiy mezonlar sifatida e'tirof etilmoqda. Xususan, kiberjinoyatchilikning latentlik darajasi an'anaviy jinoyatlarga qaraganda bir necha barobar yuqoriligi kriminolog olimlar o'rtasida keng bahslarga sabab bo'lib kelmoqda. Xususan, K. Jayshankarning «Makonlararo o'tish nazariyasi» jinoiy xulq-atvorning virtual muhitda transformatsiyalanishini shaxsning anonimlik hissi bilan bog'laydi. Jayshankar ta'kidlaganidek, "Kibermakondagi jinoiy xulq-atvor jismoniy makondan kibermakonga o'tish jarayonida shaxsning anonimlik va masofasizlik hissi ta'sirida o'zgarishi natijasidir". Biroq, ushbu yondashuvga nisbatan F. Shmallager biroz boshqacharoq munosabat bildirib, diqqatni jinoyatchi shaxsining «insonsizlashuvi» jarayoniga qaratadi. Shmallagerning fikricha, kibermakonda sub'ekt va ob'ekt o'rtasidagi jismoniy masofa ijtimoiy mas'uliyat hissini susaytiradi, bu esa jinoyatni sodir etishdagi axloqiy to'siqlarni yo'qqa chiqaradi.

Bu yerda asosiy ilmiy ziddiyat jinoyatning kelib chiqish manbaida namoyon bo'ladi: Jayshankar asosiy urg'uni makonning xususiyatiga bersa, Shmallager shaxsning psixologik holati va texnologik vositalarning ongga ta'sirini birinchi planga chiqaradi. Shu bilan birga, R. Smit ushbu bahsga texnik determinatsiya nuqtai nazaridan yondashib, latentlik muammosini ilgari suradi. Uning fikricha, texnologiyalar nafaqat jinoyat sodir etish quroli, balki "jinoyatchiga o'z izlarini yashirish uchun raqamli niqob taqdim etuvchi" vositadir. Bu yerda Smit va Jayshankarning fikrlari anonimlik masalasida tutashsa-da, Smit asosiy xavfni texnologiyaning huquqni muhofaza qilish organlaridan «tezroq» rivojlanishida ko'radi.

Transchegaraviylik masalasida esa R. Brodixerst va M. Pittaro qarashlari o'rtasidagi tahliliy farqlarni ko'rish mumkin. Brodixerst global huquq tizimidagi inqirozni va "yurisdiksiyaviy boshpanalar" muammosini ta'kidlab, milliy qonunchilikning kibermakondagi ojizligini tanqid qiladi. Undan farqli o'laroq, M. Pittaro kibertahdidlarni viktimologik jihatdan tahlil qilib, diqqatni kiberstalking kabi shaxsga yo'naltirilgan jinoyatlarning destruktiv tabiatiga qaratadi. Pittaroning fikricha, kibermakondagi tahdidlarning xavfliligi ularning hudud bilan cheklanmaganida emas, balki jinoyatchiga qurbon ustidan "doimiy va virtual nazorat o'rnatish imkonini berishidadir".

Qisqa qilib aytganda, ushbu olimlarning qarashlari bir-birini inkor etmay, balki kibermakondagi kriminologik tahdidlarning turli qirralarini ochib beradi.

Jayshankar va Shmallager jinoyatchining ichki motivatsiyasini tushuntirib bersa, Smit va Brodixerst tizimli zaifliklar hamda huquqiy prevensiyadagi bo'shliqlarni tahlil qiladi. Ushbu ilmiy konsepsiyalarning sintezi kiberjinoyatchilikka qarshi kurashda nafaqat texnik, balki chuqur nazariy-huquqiy asosga ega bo'lgan profilaktika modelini yaratish zarurligini isbotlaydi.

Ba'zi tadqiqotchilar latentlikning yuqoriligini jabrlanuvchilarning viktimologik holati va huquqni muhofaza qilish organlariga nisbatan ishonchsizligi bilan izohlasalar, boshqa bir guruh olimlar buni raqamli dalillarning tez yo'qoluvchanligi va jinoyat izlarini virtual makonda butunlay o'chirib yuborish imkoniyati mavjudligi bilan bog'laydilar. Bu yerda latentlik shunchaki statistikadagi bo'shliq emas, balki davlatning jinoyatchilik ustidan nazorati susaygan "qora hudud"ning kengayishi sifatida talqin qilinadi.

Transchegaraviylik omili esa klassik kriminologiyadagi yurisdiksiya va hududiylik tamoyillarini shubha ostida qoldirmoqda. Olimlarning ta'kidlashicha, jinoyatchi va jinoyat ob'ektining turli davlatlarda bo'lishi tergov harakatlarini nafaqat texnik, balki siyosiy-huquqiy jihatdan ham murakkablashtiradi. Bu borada ilmiy bahslar asosan raqamli suverenitet va xalqaro hamkorlik kesimida kechmoqda: bir tomon davlatlarning suveren huquqlarini ustuvor deb bilsa, ikkinchi tomon kiberjinoyatlarga qarshi kurashda chegaralarni shartli deb hisoblovchi global yurisdiksiya modelini ilgari surmoqda. Bunday vaziyatda jinoyatchilarning "huquqiy bo'shliqlar" va ekstraditsiya shartnomalari mavjud bo'lmagan davlatlardan "xavfsiz bandargoh" sifatida foydalanishi kriminal tahdidlarning global salmog'ini oshirmoqda.

Texnik determinatsiya masalasi esa jinoyat sodir etish mexanizmining tubdan intellektuallashuviga olib keldi. Kriminologlarning fikricha, bugungi kunda jinoyatchi shaxsini tavsiflashda uning jismoniy kuchi yoki ijtimoiy kelib chiqishi emas, balki texnologik bilimlari va dasturiy vositalarni boshqarish ko'nikmasi birinchi o'ringa chiqmoqda. Ilmiy munozaralarning markazida "texnologik determinizm" tushunchasi turibdi: ya'ni texnologiyalar jinoyatchilikni keltirib chiqaradimi yoki shunchaki jinoyat sodir etish uchun qulay vosita vazifasini o'taydimi? Ba'zi olimlar sun'iy intellekt va avtomatlashtirilgan algoritmlar jinoyatchilikning "insonsizlashuviga" olib kelayotganini, bu esa jinoiy javobgarlik sub'ektini aniqlashda mutlaqo yangi huquqiy muammolarni keltirib chiqarayotganini bong urmoqdalar. Shunday qilib, ushbu uchta xususiyat bir-birini to'ldirgan holda, kibermakonni an'anaviy nazorat mexanizmlaridan xoli bo'lgan, doimiy transformatsiyadagi kriminal muhitga aylantirmoqda.

Kriminologiyada kibertahdidlarning shakllanishi va rivojlanishini asoslovchi "Makonlararo o'tish" konsepsiyasi virtual va jismoniy makon o'rtasidagi

funksional farqlarni kriminologik determinatsiya nuqtai nazaridan ochib beradi. Ushbu konsepsiya doirasida shaxsning xulq-atvorini o'zgartiruvchi determinantlar o'zaro bog'liq holda jinoyat sodir etish mexanizmining tubdan transformatsiyalanishiga xizmat qiladi.

Anonimlik va shaxsiyatning moslashuvchanligi faktori kibermakonda shaxsning "dissotsiativ deingibitsiya", ya'ni ijtimoiy va axloqiy cheklovlardan voz kechish holatini keltirib chiqaradi. Jinoyatchi o'z kimligini raqamli niqoblar, shifrlangan kanallar yoki soxta profillar ortiga yashira olishi natijasida unda huquqiy javobgarlikdan qo'rqish hissi sezilarli darajada susayadi. Bu jarayonda shaxsiyatning moslashuvchanligi jinoyatchiga real hayotdagi ijtimoiy maqomidan mutlaqo farq qiluvchi «kriminal sub'ekt» qiyofasini yaratish imkonini beradi va bu holat jazoning muqarrarligi tamoyiliga nisbatan shubha uyg'otuvchi jazosizlik illyuziyasini mustahkamlaydi.

Shu bilan birga, virtual makonda ijtimoiy nazoratning pastligi jinoiy imkoniyatlar ko'lamining kengayishiga bevosita ta'sir ko'rsatadi. An'anaviy kriminologiyadagi "Kundalik faoliyat nazariyasi" kibermakonda o'zgacha shaklda namoyon bo'lib, jismoniy olamdagi jinoyat sodir etilishiga to'sqinlik qiluvchi bevosita guvohlar yoki jismoniy himoya vositalarining yo'qligi jinoyatchi uchun qulay muhit yaratadi. Bu yerdagi nazorat tizimi asosan texnik algoritmlar bilan cheklangan bo'lib, ular jinoiy maqsadlarni amalga oshirishda inson omili kabi to'sqinlik qila olmaydi, natijada jinoyatchi va qurbon o'rtasidagi masofaning yo'qligi jinoiy hujumlarning global miqyosda va kam xavf bilan amalga oshirilishiga yo'l ochadi.

Mazkur jarayonning mantiqiy davomi sifatida normativ ziddiyatlar va huquqiy nigilizm muammosi yuzaga keladi. Shaxsning real ijtimoiy muhitda shakllangan axloqiy me'yorlari kibermakonning chegarasiz virtual erkinligi bilan to'qnashganda, shaxs ongida normativ bo'shliq shakllanadi. Ko'p hollarda kibermakondagi destruktiv harakatlar, masalan kiberta'qib yoki boshqa shaxsning huquqlarini buzish, sub'ekt tomonidan jiddiy huquqbuzarlik sifatida emas, balki "raqamli erkinlik"ning bir ko'rinishi sifatida qabul qilinadi. Bunday yondashuv kibermakondagi jinoiy qilmishlarni psixologik jihatdan legitimlashtirishga va jinoyatchilikning oldini olishdagi ma'naviy-huquqiy to'siqlarning yemirilishiga olib keladi, bu esa o'z navbatida kiberjinoyatchilikning tizimli ravishda o'sishini ta'minlovchi determinant bo'lib xizmat qiladi.

Zamonaviy kibertahdidlar tizimida qurbonning xulq-atvori, ya'ni viktimologik jihatlari jinoyat mexanizmining ajralmas bo'lagi sifatida namoyon bo'lmoqda. Xususan, Web 2.0 va Web 3.0 texnologiyalari foydalanuvchilarga nafaqat axborot iste'mol qilish, balki o'z shaxsiy hayotiga doir ma'lumotlarni

chegarasiz miqdorda ochiqlash imkonini taqdim etdi. Bu esa kriminologik nuqtai nazardan jinoyatchilar uchun bepul va ochiq «intellektual razvedka» manbaini shakllantirib, potensial qurbonni tanlash va uning ustidan nazorat oʻrnatish jarayonini avtomatlashtirdi. Foydalanuvchi tomonidan ijtimoiy tarmoqlarga joylashtirilgan geopozitsiyalar, fotosuratlar va shaxsiy qiziqishlar jinoyatchiga qurbonning kundalik harakat traektoriyasini aniqlash va masofaviy taʼqibni boshlash uchun zarur boʻlgan barcha detallarni taqdim etadi.

Ayniqsa, kiberstalking va kiberbulling kabi tahdidlar shaxsning ruhiy daxlsizligiga tizimli ravishda zarba berib, uning ijtimoiy izolyatsiyasiga va psixologik degradatsiyasiga sabab boʻladi. Ushbu jinoyatlarning anʼanaviy taʼqibdan farqi shundaki, virtual olamda tahqirlash soniyalar ichida global miqyosga chiqishi va qurbonni sutkasiga 24 soat davomida taʼqib qilishi mumkin. Bunday “raqamli panoptikum” holati jabrlanuvchida doimiy xavotir va qoʻrquv hissini uygʻotib, uni jamiyatdan uzilishiga va virtual olamdagi ijtimoiy maqomining yoʻqolishiga olib keladi. Natijada, kibermakon shaxs uchun xavfsiz muloqot maydonidan psixologik zoʻravonlik poligoniga aylanadi.

Bu borada voyaga yetmagan yoshlarning onlayn muhitdagi faolligi ularning viktimizatsiya darajasini keskin oshiruvchi eng xavfli omillardan biri hisoblanadi. Yosh avlodning raqamli olamdagi tajribasizligi, ishonuvchanligi va shaxsiy maʼlumotlar daxlsizligi borasidagi bilimlarining yetishmasligi ularni onlayn jinsiy yirtqichlar va ekspluatatsiya qiluvchi subʼektlar uchun eng oson nishonga aylantiradi. Kriminologik tadqiqotlar shuni tasdiqlaydiki, voyaga yetmaganlarning raqamli izlari ularning kelajakdagi ijtimoiy hayoti va xavfsizligiga taʼsir etuvchi “viktimologik zahira” boʻlib xizmat qilmoqda. Shu sababli, kibermakondagi viktimlikni kamaytirish uchun nafaqat texnik cheklovlar, balki yoshlarda kriminologik immunitetni shakllantirish va raqamli gigiena madaniyatini tizimli ravishda singdirish davlatning huquqiy siyosatidagi ustuvor yoʻnalish boʻlishi lozim.

Kibermakondagi jinoyatchilikning transformatsiyasi va uning determinatsiyasi tahlili shuni koʻrsatadiki, anʼanaviy kriminologik choralar raqamli makondagi tahdidlarga qarshi kurashda yetarli samara bermayapti. Jinoyatchilikning yuqori darajadagi latentligi va transchegaraviy tabiati davlatning jinoiy-huquqiy siyosatini yangicha yondashuvlar asosida qayta koʻrib chiqishni taqozo etadi. Yuqoridagilardan kelib chiqib, quyidagi ilmiy-amaliy takliflar ilgari suriladi:

1. Jinoiy qonunchilikni tizimlashtirish va kvalifikatsiya mezonlarini aniqlashtirish. Oʻzbekiston Respublikasi Jinoyat kodeksining axborot texnologiyalari sohasidagi jinoyatlarga oid normalarini (XX¹ bob) zamonaviy

kibertahdidlar, xususan, kiberstalking va kiberbulling kabi qilmishlar uchun alohida kvalifikatsiya belgilari bilan to'ldirish lozim. Bunda shaxsning ruhiy daxlsizligiga raqamli vositalar orqali yetkazilgan zarar uchun jinoiy javobgarlikni differentsiatsiya qilish muhim ahamiyatga ega. Bu huquqni muhofaza qilish organlariga qilmishni to'g'ri baholash va jazoning muqarrarligini ta'minlash imkonini beradi.

2. Raqamli viktimologik profilaktika tizimini joriy etish. Kibermakondagi viktimlik darajasini kamaytirish maqsadida davlat miqyosida "Raqamli gigiena va kiberxavfsizlik" milliy dasturini ishlab chiqish zarur. Ushbu dastur doirasida ta'lim muassasalarida yoshlarning kriminologik immunitetini oshirishga qaratilgan maxsus kurslarni joriy etish, foydalanuvchilarga o'z shaxsiy ma'lumotlarini himoya qilish va manipulyatsiyalarni aniqlash ko'nikmalarini o'rgatish lozim. Bu jinoyatchilar uchun "intellektual razvedka" maydonini toraytirishga xizmat qiladi.

3. Protsessual harakatlarni raqamlashtirish va elektron dalillar institutini mustahkamlash. Kiberjinoyatlarni tergov qilish samaradorligini oshirish uchun Jinoyat-protsessual kodeksida "elektron dalil" tushunchasini va uni to'plash, saqlash hamda taqdim etishning aniq protsessual tartibini belgilash kerak. Raqamli izlarning tez yo'qoluvchanligini inobatga olib, tezkor-qidiruv tadbirlari davomida elektron ma'lumotlarni kechiktirib bo'lmaydigan tartibda fiksatsiya qilishning huquqiy mexanizmlarini takomillashtirish lozim.

4. Xalqaro hamkorlik va "yurisdiksiyaviy boshpanalar"ga barham berish. Kiberjinoyatchilikning transchegaraviyligini inobatga olib, kibermakondagi jinoyatlar bo'yicha elektron dalillar bilan tezkor almashish va jinoyatchilarni ekstraditsiya qilish bo'yicha xalqaro shartnomalar tarmog'ini kengaytirish zarur. Bunda Budapesht konvensiyasi kabi xalqaro standartlar asosida milliy qonunchilikni muvofiqlashtirish va mintaqaviy kiberxavfsizlik markazlari bilan tezkor aloqalarni yo'lga qo'yish tavsiya etiladi.

5. Huquqni muhofaza qilish organlari xodimlarining texnologik kompetensiyasini oshirish. Kibermakondagi tahdidlarni aniqlash va ularga qarshi kurashish uchun ichki ishlar va prokuratura tizimida yuqori texnologik bilimlarga ega bo'lgan "kiber-kriminolog" va "raqamli detektiv" mutaxassislarini tayyorlash tizimini yo'lga qo'yish lozim. Jinoyatchilikning texnik determinatsiyasiga javoban, davlat organlarining texnik nazorat va monitoring imkoniyatlarini doimiy ravishda yangilab borish strategik vazifa hisoblanadi.

FOYDALANILGAN ADABIYOTLAR RO'YXATI:

1. Broadhurst, R. (2006). Developments in the global law enforcement of cyber-crime. *Policing: An International Journal of Police Strategies & Management*, 29(3), 408–433. <https://doi.org/10.1108/13639510610684674>
2. Grabosky, P. N. (2016). *Cybercrime*. Cambridge University Press.
3. Jaishankar, K. (2007). Establishing a General Theory of Cyber Crime. *International Journal of Cyber Criminology*, 1(1), 7–9.
4. Jaishankar, K. (2008). Space Transition Theory of cyber crimes. In F. Schmallegger & M. Pittaro (Eds.), *Crimes of the Internet* (pp. 283–301). Prentice Hall.
5. Kshetri, N. (2010). *The Global Cybercrime Industry: Economic, Institutional and Strategic Perspectives*. Springer Science & Business Media.
6. Pittaro, M. L. (2007). Cyber stalking: An analysis of online harassment and intimidation. *International Journal of Cyber Criminology*, 1(2), 180–197.
7. Schmallegger, F., & Pittaro, M. (2008). *Crimes of the Internet*. Prentice Hall.
8. Smith, R. G., Grabosky, P. N., & Urbas, G. (2004). *Cyber Criminals on Trial*. Cambridge University Press.
9. Wall, D. S. (2007). *Cybercrime: The Transformation of Crime in the Information Age*. Polity Press.
10. Yar, M., & Steinmetz, K. F. (2019). *Cybercrime and Society* (3rd ed.). SAGE Publications.

МИЛЛИЙ ҚОНУНЧИЛИК ВА МАНБАЛАР:

11. Ўзбекистон Республикасининг Жиноят кодекси. (1994 йил 22 сентябрь). Ўзбекистон Республикаси Қонунчилик маълумотлари миллий базаси.
12. Рустамбаев, М. Х. (2021). *Криминология: Умумий қисм* (Дарслик). Тошкент давлат юридик университети.